Be Suspicious about Trusting Unauthenticated External Representation of Internal Data Structures

William L. Fithen, Software Engineering Institute [vita[3]]

2005-10-03

Trusting unauthenticated externalized data structures can introduce vulnerability.

Description

Many systems depend on technologies that support the rendering of internal data structures or objects into the form of *serial streams* of bytes. These external representations are used for a variety of functions, including mobile objects, distributed objects, and remote procedure calls. When an adversary can modify the serial stream between its time of production and later use, a vulnerability may exist. Four different situations can cause vulnerability:

- If the altered serial stream is syntactically invalid, blind restoration of the serial stream can result in a variety of vulnerabilities, the most frequent being buffer overflow.
- If the altered serial stream is syntactically invalid and the restoring program recognizes this, it will not restore the stream, avoiding more serious vulnerabilities but perhaps still resulting in a denial of service.
- If the altered serial stream is syntactically valid but semantically invalid, restoration of the serial stream results in a valid internal representation of data structures or objects, but those structures or objects are not what the original serializing program intended to have restored. This can result in a variety of erroneous or vulnerable behaviors.
- If the altered serial stream is syntactically valid but semantically invalid and the restoring program recognizes this, it will not restore the stream, avoiding more serious vulnerabilities but perhaps still resulting in a denial of service.

References

[VU#192995]	Havrilla, Jeffrey. *Vulnerability Note VU#192995: Integer overflow in xdr_array() function when deserializing the XDR stream*. http://www.kb.cert.org/vuls/id/192995 (2005).
[VU#597889]	Dougherty, Chad. *Vulnerability Note VU#597889: Microsoft COM Structured Storage Vulnerability*. http://www.kb.cert.org/vuls/id/597889 (2005).

SEI Copyright

[3] daisy:320 (Fithen, William L.)

Felder

Name	Wert
Copyright Holder	SEI

Felder

Name	Wert
is-content-area-overview	false
Content Areas	Knowledge/Guidelines
SDLC Relevance	Implementation
Workflow State	Publishable

[1] http://www.sei.cmu.edu/about/legal-permissions.html